UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FAN MILLS, individually and behalf of all others similarly situated,

Plaintiff,

-against-

SAKS.COM LLC,

Defendant.

Case No. 1:23-cv-10638 (ER)

ORAL ARGUMENT REQUESTED

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT

LOEB & LOEB LLP
Christopher A. Ott (admitted *pro hac vice*)
901 New York Ave NW
Suite 300 East
Washington, DC 20001
Tel: (202) 618-5000

Christian D. Carbone
Elena De Santis
345 Park Avenue
New York, NY 10154
Tel: (212) 407-4000

Attorneys for Defendant Saks.com LLC

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Defendant Saks.com LLC ("Saks"), by and through its counsel, Loeb & Loeb LLP, respectfully submits this memorandum of law in support of its motion to dismiss Plaintiff's First Amended Complaint (Dkt. No. 29, "FAC"), and all claims asserted therein pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6).

PRELIMINARY STATEMENT

In this action, Plaintiff attempts to expand the scope of a seventeen-year-old Arizona statute well beyond its terms and intended scope, to hold Saks liable for using the functional equivalent of a "read receipt" in its own marketing emails. The FAC—a virtual copy and paste of others simultaneously filed by Plaintiff's counsel—alleges that Saks (1) utilizes "pixels" in its marketing emails, which track when users open and read an email (*i.e.*, a read receipt), along with the email address and the subject of Saks' marketing email; and (2) includes such "tracking pixels" within images embedded within its emails through the use of Adobe pixels, which, per Plaintiff, allegedly track recipient activity, such as when the emails are opened and whether links are clicked. This read-receipt technology is so ubiquitous that nearly every email service offers it.

Plaintiff asks this Court, in a case of first impression, to apply an expansive interpretation of the Arizona Telephone, Utility and Communication Service Records Act, A.R.S. § 44-1376 (the "Arizona Statute" or "Statute") without any case law support. Under any theory that Plaintiff asserts, and even after amending her complaint, the FAC still fails to alleges facts sufficient to establish Article III standing, and facts sufficient to state a claim under the Arizona Statute, and should be dismissed for at least the following reasons:

First, Plaintiff lacks Article III standing because she fails to make the threshold showing that she has suffered an injury in fact that is concrete, particularized, and actual or imminent. Plaintiff does not allege any monetary, physical, or other tangible injury. Because Plaintiff has

not alleged an invasion of privacy on Saks' part that would be highly offensive to a reasonable person—or other harm that has been traditionally recognized as providing a basis for a lawsuit—she has likewise failed to allege a concrete intangible injury. Given that Plaintiff fails to allege any concrete harm at all, let alone a concrete injury beyond a bare statutory violation, she cannot establish Article III standing to pursue her claims.

Second, the FAC fails to state a claim under the Arizona Statute because Saks did not collect a "communication service record," the specific information the Arizona Statute protects. Any information Saks collected about the Plaintiff was (i) necessarily incident to Saks' rendering of services; and/or (ii) was collected consistent with Saks' publicly posted Privacy Policy and without any fraudulent, deceptive or false means. Plaintiff's expansive interpretation is also inconsistent with other courts' interpretations of analogous statutes.

Third, Plaintiff's expansive interpretation of the Arizona Statute is inconsistent with both the Statute's legislative intent and legislative history, both of which focused on preventing unauthorized disclosures of personal information through pretextual and fraudulent means.

No case has ever applied the Arizona Statute to impose liability for an entity's use of "spy pixels" as plaintiff urges. For the reasons discussed herein, this Court should not be the first, especially when Plaintiff's suggested application unduly expands the scope of the Statute and would produce an absurd result. Allowing Plaintiff's expansive interpretation to prevail would render the publicly disclosed use of read-receipt technology, which is ubiquitous and necessary in both digital marketing practices and email services generally, unlawful. This is a far cry from what the Arizona Statute was enacted to prevent, and Plaintiff's counsel should not be permitted to rewrite the Statute through one of its several copycat litigations—none of which is even proceeding in Arizona state court. The FAC should be dismissed in its entirety, with prejudice.

FACTUAL BACKGROUND[1]

I. HP's Use of Pretexting and Lawmakers' Responses

In a perplexing non-sequitur, the bulk of the FAC discusses a series of "leaks" of information at Hewlett Packard ("HP") in the early 2000s, and the Company's responses thereto. FAC ¶¶ 15-28. The conversations that were leaked contained sensitive and confidential information, and included information on the then-CEO Carly Fiorina losing the confidence of the board of directors, HP's phasing her out of the CEO position, and HP's choice of a replacement CEO from a purported competitor. *Id.* ¶¶ 17, 20. Given the sensitivity of the leaked information, HP conducted two investigations into the sources and scope of the leaks. *Id.* ¶¶ 20-23.

HP's investigation tactics were eventually made public, which led to a Congressional hearing on the matter. *Id.* ¶¶ 25-26. The Congressional hearing and related publicity revealed that HP and its investigators used multiple tactics to investigate the source of the leaks. The first, pretexting, "involved investigators requesting information from [telephone] operators orally, over the phone, pretending to be someone else if necessary." *Id.* ¶ 21 (citation omitted). In addition to pretexting over the phone, HP's investigators *de facto* pretexted over email, as well. Like traditional pretexting, HP investigators "pos[ed] as a disgruntled employee" and "emailed [the journalist] with the promise of revealing damaging information about the company." *Id.* ¶ 23. HP utilized a software called "ReadNotify," which, once embedded into an email, allowed HP to "track the path [the] message takes, including whether [the] recipient opens the message," critically, in hopes that the journalist would ***forward the email to her source*** "thereby revealing who had leaked the confidential information." *Id.* ¶ 23.

[1] These facts and allegations are taken from the FAC.

HP's use of pretexting became the impetus for Congress enacting the Telephone Records and Privacy Protection Act of 2006 (the "TRPPA") and for the Arizona legislature to enact the Arizona Telephone, Utility and Communication Service Records Act, A.R.S. § 44-1376. While the TRPPA criminalizes "knowingly and intentionally obtain[ing], or attempt[ing] to obtain, confidential phone records information . . . by making false or fraudulent statements or representations to an employee of a covered entity" (*id.*¶ 27), the Arizona Statute extends its prohibitions beyond telephone records and prohibits the procurement of any "communication service record" of any Arizona resident "without the authorization of the customer to whom the record pertains, or by fraudulent, deceptive or false means. *Id.* ¶ 28.

II. Plaintiff's Allegations as to Saks

Plaintiff's recitation of the HP scandal is noteworthy, as it shows the kind of practices that the Arizona Statute was intended to prohibit. In contrast to Plaintiff's detailed recitation of the HP pretexting scandal, Plaintiff's allegations against Saks barely state that Plaintiff is a resident of Arizona who has "frequently opened emails from Defendant to review promotion materials" between 2017 to October 2023. FAC ¶¶ 7-8. Plaintiff alleges that each time she opened an email, Saks "procured information identifying her and disclosing when she opened and read the email," without her consent to do so. *Id.* ¶¶ 9-10, 30, 32. Plaintiff previously advised the Court that the software telling Saks whether she opened the email is itself a violation of the Arizona Statute. *See* Transcript of Teleconference, dated Mar. 20, 2024, at 5:11-19.[2]

Per the FAC, Saks obtained this information through its use of email pixels, which Plaintiff describes as a 1x1 (one pixel high by one pixel long) image, which is "basically impossible to see

[2] A copy of the transcript of the pre-motion conference is annexed to the accompanying Declaration of Christopher A. Ott (the "Ott Decl.") as Exhibit A.

with the naked eye" and activated by opening an email. FAC ¶ 33. Plaintiff contends that Saks uses the pixel software in its marketing emails to log when the recipients access the email, the number of times the email is opened, and the user's IP address. *Id.* ¶ 30. Plaintiff now alleges that Saks utilizes pixels within images embedded within its marketing emails, through the use of Scene 7, an Adobe subsidiary. *Id.* ¶ 38. The information purportedly collected by the Adobe software is similar to the information Plaintiff otherwise alleges is collected by the email pixels, including information on opens and subsequent clicks. *Id.* ¶ 41. Yet in discussing the information the Adobe software can purportedly collect, Plaintiff does not link such allegations to Saks. Instead, Plaintiff includes a graphic and accompanying allegations that are not particular to Saks, but rather an exact copy-paste of a generalized example from an Adobe Website. *Id.* ¶ 41, n.60.

The FAC later alleges that "the spy pixels are designed to extract 'communication service records'" including "time logs of email access, logs of associated email addresses, logs of email client type, logs of email path data, logs of recipient location, logs of IP addresses, logs of email forwarding data, and logs of device information." *Id.* ¶ 55. Plaintiff similarly fails to indicate whether the "spy pixels" discussed in Paragraph 55 are those purportedly utilized by Saks, or "spy pixels" generally.

To even receive such marketing emails from Saks—and images embedded within those emails—an individual user must either make an online purchase from Saks and consent to receive promotional materials, or otherwise create an online account with Saks, which requires the user to provide their first name, last name, and email address. Every user agrees to Saks' Privacy Policy and Terms and Conditions whenever they access the website, and again when they create an

account.[3] Saks' Privacy Policy discloses that Saks may use pixel tags or other technologies to collect certain information about visitors to its website or interactions with emails and online advertisements.

ARGUMENT

I. Legal Standards

Defendant brings this motion pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). In such cases, the Court must consider the Rule 12(b)(1) motion first because "disposition of a Rule 12(b)(6) motion is a decision on the merits, and therefore, an exercise of jurisdiction." *See Gannon v. 31 Essex St. LLC*, No. 22-cv-1134 (ER), 2023 U.S. Dist. LEXIS 7873, at *4 (S.D.N.Y. Jan. 17, 2023) (quoting *Chambers v. Wright,* No. 5 Civ. 9915 (WHP), 2007 U.S. Dist. LEXIS 92729, at *4 (S.D.N.Y. Dec. 19, 2007)).

Pursuant to Fed. R. Civ. P. 12(b)(1), a complaint must be dismissed for lack of subject matter jurisdiction when the district court lacks the statutory or constitutional power to adjudicate it, "such as when (as in the case at bar) the plaintiff lacks constitutional standing to bring the action." *See Cortlandt St. Recovery Corp. v. Hellas Telecomms.*, 790 F.3d 411, 417 (2d Cir. 2015) (internal citations omitted). Plaintiff bears the burden of establishing that she has standing to sue. *See id.* To meet her burden for the "irreducible constitutional minimum" of Article III standing

[3] Saks' website's Terms and Conditions explicitly incorporate the Privacy Policy. *See* Saks Fifth Avenue, "Terms and Conditions," https://www.saksfifthavenue.com/c/content/terms-and-conditions; Saks Fifth Avenue, "Saks Fifth Avenue Privacy Policy," https://www.saksfifthavenue.com/c/content/privacy-policy. Because the Terms and Conditions and Privacy Policy are posted publicly on Saks.com and their authenticity is not in question, the Court may take judicial notice of the contents Saks' website. *See Zambrano v. Strategic Delivery Sols., LLC*, No. 15. Civ. 5410 (ER), 2022 U.S. Dist. LEXIS 146669, at *4 n.3 (S.D.N.Y. Aug. 16, 2022) (citing *Force v. Facebook, Inc.*, 934 F.3d 53, 59 n.5 (2d Cir. 2019) (taking judicial notice of contents of Facebook's terms of service)). True and correct copies of Saks.com's Terms and Conditions and Privacy Policy are annexed Ott Declaration as Exhibits B and C.

(*see Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992)), Plaintiff must demonstrate that she "(i) suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 594 U.S. __, __, 141 S. Ct. 2190, 2203 (2021) (citing *Lujan*, 504 U.S. at 560-61). Because Plaintiff has failed to demonstrate injury in fact, she lacks Article III standing to pursue her claim and the FAC must be dismissed for lack of subject matter jurisdiction.

To survive a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6), a complaint must contain "factual allegations sufficient 'to raise a right to relief above the speculative level.'" *ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct," dismissal is appropriate. *Nielsen v. AECOM Tech. Corp*, 762 F.3d 214, 218 (2d Cir. 2014) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009)). Although a court will assume well-pled factual allegations to be true on a motion to dismiss, the same assumption does not extend to legal conclusions. *See Golden v. NBCUniversal Media, LLC*, No. 22 Civ. 9858 (PAE), 2023 U.S. Dist. LEXIS 150622, at *6 (S.D.N.Y. Aug. 23, 2023). "Pleadings that offer only 'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not do.'" *Id.* (quoting *Twombly,* 550 U.S. at 555).

II. Plaintiff Lacks Article III Standing to Assert Her Claims

Plaintiff fails to make the threshold showing that she has suffered an injury in fact sufficient to establish Article III standing, which requires that Plaintiff "(i) suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion*, 141 S. Ct. at 2203 (citing *Lujan*, 504 U.S. at 560-61). The FAC alleges that Saks (the sender of the

email) used pixels—through the email itself or embedded images—to collect Plaintiff's email address (which Plaintiff had previously provided to Saks), the subject of the email (which Saks sent), and read-receipt confirmation of that same email message. Unlike the HP matter that the Complaint discusses at length, no broader invasion of privacy is alleged or even implied, and Plaintiff's colorful conclusory language regarding "invasive surveillance" and "clandestine collection" (FAC ¶ 5) fall far short of being particularized or concrete. For an injury to be particularized, it "must affect the plaintiff in a personal and individual way, *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (quoting *Lujan*, 504 US. at 560 n.1), but the injury must also be concrete. The fact of a read-receipt, without more, cannot be concrete. In the absence of certain tangible harms, such as physical harms and monetary harms, that "something more" must be alleged.

Spokeo acknowledged that certain intangible harms could also be sufficiently concrete only if they have a "close relationship to a harm that has traditionally been regarded as providing a basis for lawsuits in . . . American courts." *Spokeo*, 578 U.S. at 340-41. However, the fact that Congress—or here, the Arizona state legislature—may have identified and elevated an intangible harm "does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Id.*, 578 U.S. at 341. Even if the Arizona Statute applies, and it does not, these facts allege at most benign technical harm—a sender receiving a "read receipt" notification—that a reasonable person would rightly consider inoffensive or innocuous. As the Court in *Spokeo* recognized, a plaintiff "could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III." *Id.* This is precisely what Plaintiff has done in her FAC, and even before *TransUnion*, such benign technical harm would not establish Article III standing.

The *TransUnion* Court further clarified that the harm must extend beyond the statute itself. While Congress's views may be "instructive" in determining whether a harm is concrete, the Court explicitly held that "under Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court." *TransUnion,* 141 S. Ct. at 2205. As the Second Circuit has recognized, the Supreme Court's decision in *TransUnion* "narrowed the grounds for asserting standing where the injury is primarily statutory." *See Faehner v. Webcollex, LLC*, No. 21-cv-1734, 2022 U.S. App. LEXIS 4439, at *1 (2d Cir. Feb. 18, 2022). Indeed, per the Second Circuit, "the Supreme Court clarified that a plaintiff has standing to bring a claim for monetary damages following a statutory violation ***only when he can show a current or past harm beyond the statutory violation itself.***" *Harty v. West Point Realty, Inc.*, 28 F.4th 435, 443 (2d Cir. 2022) (emphasis added); *see also Maddox v. Bank of N.Y. Mellon Trust Co., N.A.*, 19 F.4th 58, 64 (2d Cir. 2021) (recognizing that Plaintiff cannot establish Article III standing by relying entirely on a purported statutory violation: "No concrete harm; no standing.") (quoting *TransUnion*, 141 S. Ct. at 2214)).

The FAC's bare allegation that Defendant's "clandestine collection of [] confidential email records also intruded upon their seclusion" (FAC ¶ 61), and Plaintiff's addition of "logs" before the information purportedly collected still fail to establish (1) that Plaintiff suffered such a concrete injury; or (2) that the alleged harm caused by a read receipt bears a close relationship to harm suffered from intrusion upon seclusion. Although courts have recognized the tort of intrusion upon seclusion as an example of an "intangible harm[] [that] can also be concrete," *TransUnion LLC*, 141 S. Ct. at 2204, integral to such claims is an invasion that would be "highly offensive to a reasonable person." *See, e.g.*, *Six v. IQ Data Int'l Inc.*, No. CV-22-00203-PHX-MTL, 2023 U.S.

Dist. LEXIS 87593, at *7 (D. Ariz. May 18, 2023) (quoting Restatement (Second) of Torts § 652B (1977)); *Ciccone v. Cavalry Portfolio Servs., LLC,* Nos. 21-cv-2428 (JS)(JMW) and 21-cv-3764 (JS)(AYS), 2021 U.S. Dist. LEXIS 228037, at *10 (E.D.N.Y. Nov. 29, 2021) (applying *TransUnion* and finding that an alleged statutory violation based on the disclosure to third-parties of plaintiffs' names, addresses, status as debtors, and the precise amounts of their alleged debts did not amount to a concrete injury because, as here, the disclosure would not be highly offensive to a reasonable person). These cases support the fact that something more than collecting data on whether an email has been opened and read, or whether links have been clicked, must be alleged for standing to exist.

For example, the *Six v. IQ* case discusses how the intrusion upon seclusion tort seeks to guard against invasion of privacy by some "form of investigation or examination into [one's] private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents." *Id.* at *9 (citation omitted). However, on the face of the FAC, Saks.com's actions are not equivalent to opening Plaintiff's mail or other conduct that courts have found to trigger non-frivolous privacy concerns. S*ee also In re: BPS Direct, LLC, MDL 3074*, 2023 U.S. Dist. LEXIS 216728, at *33-34, *41 (E.D. Pa. Dec. 5, 2023) (plaintiffs' allegations that the website operators secretly tracked their keystrokes and browsing activity while on the operators' websites were dismissed for lack of subject matter jurisdiction because the website users had failed to allege that the website operators captured anything other than their browsing activity and held that "browsing activity is not sufficiently private to establish concrete harm . . . . [as well as] viewing activity, search activity, and purchase behavior is [not] enough to establish concrete harm.").

In the instant case, Plaintiff conclusorily refers to the information purportedly collected as "confidential," but fails to show that the information purportedly procured is sensitive, private, or confidential, let alone provide plausible allegations that such procurement would be highly offensive to a reasonable person. *See Aponte v. Ne. Radiology, P.C.*, No. 21-cv-5883 (VB), 2022 U.S. Dist. LEXIS 87982, at *11 (S.D.N.Y. May 16, 2022); *see also I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (holding that alleged privacy injuries were not sufficiently concrete to confer Article III standing because "the Court [did] not view the collection of email addresses, phone numbers, Zynga usernames, Zynga passwords, and Facebook usernames [to be] so private that their revelation would be highly offensive to a reasonable person"). Notably, the FAC does not allege that any other private or sensitive information about Plaintiff was communicated. Instead, the FAC merely alleges that Saks.com, with which Plaintiff had already opened an account, received confirmation that she had opened the email and confirmation as to whether she had clicked on any links embedded within the email that she signed up for.

These bare allegations implicate no sensitive data or information. For this reason, Plaintiff cannot point to any analogous privacy tort. Because a "key element of the analogous common-law or historical harm is missing, the plaintiff lacks standing" to pursue her claims. *Sputz v. Alltran Fin., LP*, No. 21-cv-4663 (CS), 2021 U.S. Dist. LEXIS 233292, at *7 (S.D.N.Y. Dec. 5, 2021) (quoting *Age Kola v. Forster & Garbus LLP,* No. 19-cv-10496 (CS), 2021 U.S. Dist. LEXIS 172197, at *15 (S.D.N.Y. Sept. 10, 2021).

Because Plaintiff has not alleged a concrete injury, she has failed to allege injury in fact. Accordingly, Plaintiff lacks Article III standing to pursue her claim, and the FAC must be dismissed for lack of subject matter jurisdiction.

III. Plaintiff Fails to State a Claim Under the Arizona Statute

A. Plaintiff Does Not Allege Sufficient Facts to Sustain a Clam for Relief

Even if Plaintiff had standing to bring her claim (which she does not), the FAC still fails as a matter of law because Plaintiff has failed to state a claim for relief under the Arizona Statute. In support of her sole claim, Plaintiff recites the elements of the Arizona Statute, and alleges that she has opened an unspecified number of emails from Saks over the past seven years.[4] FAC ¶¶ 7-9, 55-56. Although well-pled factual allegations are accepted as true, this principle is "inapplicable to threadbare recitals of a cause of action's elements, supported by mere conclusory statements." *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009); *see also Conklin v. Maidenbaum*, No. 12-cv-3606 (ER), 2013 U.S. Dist. LEXIS 113975, at *12-13 (S.D.N.Y. Aug. 13, 2013) ("Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief.").

There is no case law interpreting these provisions of the Arizona Statute at all, much less case law favoring Plaintiff's expansive interpretation of the Statute. Accordingly, there is no authority characterizing the terms of the provisions at issue as clear or unambiguous. However, Plaintiff's claim still fails for several reasons.

As a preliminary matter, the information purportedly collected by Saks does not fall within the information protected by the Arizona Statute, namely communication service records. *First*, "information about when and whether a customer opens and reads an email" (FAC ¶ 36), and "statistics on opens, clicks and transactions," and "the list of pages visited following a delivery" (*id.* ¶ 40) are not included in the definition of "communication service record." *See Kidd v.*

[4] To the extent the FAC purports to press claims based on statutory violations as far back as 2017, a two-year statute of limitations bars any claims based on these older alleged violations. A.R.S. § 44-1376.04(B).

Thomson Reuters Corp., 925 F.3d 99, 106 n.9 (2d Cir. 2019) (noting that where a "statute does not include this language" a court "may not 'add words to the law to produce what is thought to be a desirable result'") (citation omitted).

Second, to the extent Plaintiff alleges that Saks collected her email address and other information through the pixels, it was through an email sent *by* Saks, not one created by Plaintiff; in other words, Plaintiff had previously provided her email address and contact information to Saks. This reinforces the fact that the pixels—to the extent they were used—were functioning as read receipts, rather than a purported collection of Plaintiff's personally identifiable information. Moreover, this again differentiates these allegations from the HP procedural history that makes up the bulk of the complaint, wherein the bad actors sought to recover information beyond merely reading the email and clicking on links therein.

Third, and importantly, the statute prohibits the procurement of "records of the path of an electronic communication between the point of origin and the point of delivery[.]" *See* A.R.S. §§ 44-1376(1) and 44-1376.01. However, Plaintiff alleges that the pixels record whether Saks' email has been opened and read, or whether links have been clicked and other data, ***after*** the delivery, rather than the path of the communication between the point of origin (Saks) and the point of delivery (the Plaintiff). *See* FAC ¶¶ 36, 40. Based on the plain terms of the Arizona Statute, such data does not fall within the Statute's ambit.

Even if we assume for the purposes of this motion that Saks did procure "communication service records," the Arizona Statute "does not prohibit . . . an entity that maintains communication service records from obtaining, using, disclosing or permitting access to any . . . communication service record either directly or through its agents" "[a]s may be necessarily incident to the rendition of the service[.]" *See* A.R.S. § 44-1376.02(B)(3). As disclosed in its Privacy Policy (*see*

Ott Decl. Ex. C), Saks may use the information collected as necessary to, *inter alia*, validate, deliver, and track customers' orders; to enhance customers' online shopping experience; and to measure and improve the effectiveness and performance of Saks' sites, products and services, and customer service, each of which is integral to and necessary for Saks to maintain its online shopping platform.

Plaintiff's claim additionally fails because any procurement of information was not done "without the authorization of the customer to whom the record pertains or by fraudulent, deceptive or false means." *See* A.R.S. § 44-1376.01(A)(1). The FAC still ignores the fact that when an individual accesses Saks' website or creates an online account with Saks, they agree to Saks' Terms and Conditions, including Saks' Privacy Policy. The first question within the Privacy Policy's Q&A is "**What information does Saks collect?**" *See* Ott Decl. Ex. C at 1-2 (emphasis in original). As relevant here, the Privacy Policy explicitly informs users that it "may use cookies, web beacons, javascript and pixel tags, log files, or other technologies" to collect information about visitors to Saks.com or users of Saks' services, including "information such as your browser type, operating system type or mobile device model, viewed webpages, **links that are clicked**, IP address, mobile device identifier or other unique identifier, sites or apps visited . . . [and] **emails we send that you open, forward, or click through to our Site or App.**" *Id.* at 2 (emphasis added). Where, as here, the existence of the terms was reasonably communicated to the user, courts have found such agreements valid. *See Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 76 (2d Cir. 2017).

Because Saks did not collect the information covered by the Statute, and any information collected was (1) necessarily incident to Saks' rendering of services; and/or (2) not done without

Plaintiff's authorization or by fraudulent, deceptive or false means, Plaintiff has not stated a claim under the Statute, and the FAC should be dismissed.

B. Plaintiff's Expansive Interpretation of the Arizona Statute is Inconsistent with Courts' Interpretations of Other Analogous Statutes

Although no court has addressed the issues presented by the Arizona Statute as alleged in the FAC, other courts' interpretations of analogous statutes can provide direction. In a case of first impression, where "[t]here does not appear to be any Arizona case law on point," Arizona courts "look for guidance [from] other jurisdictions that have addressed [the] issue." *See Sprint Commc'ns Co. v. W. Innovations, Inc.*, 618 F. Supp. 2d 1124, 1125 (D. Ariz. 2009) (citation omitted).

Plaintiff alleges that the pixels record whether an email recipient has opened and read an email after delivery, and whether any embedded links are clicked on after opening the email, and contends that this is sufficient to state a violation under the Arizona Statute. Besides not falling within the definition of "communication service records," Plaintiff's allegations would similarly fail under analogous statutes barring the interception of data "in transit." Just as the Arizona Statute's definition of "communication service record" requires "the path of an electronic communication [to be] ***between the point of origin and the point of delivery***" (A.R.S. § 44-1376(1) (emphasis added)), courts interpreting analogous wiretap statutes have required that the communication be intercepted "in transit," *i.e.*, "during the communication's transmission and not during electronic storage." *See, e.g.*, *Licea v. Cinmar, LLC*, 659 F. Supp. 3d 1096, 1109-1110 (C.D. Cal. 2023). The court in *Licea* found that the communication was not intercepted "in transit" under the California Invasion of Privacy Act because the plaintiff's allegations were "conclusory and [did] not allege specific facts as to how or when the interception takes place." *Id.* The same result should apply to Plaintiff's conclusory allegations here.

Other courts have rejected claims arising out of the same kinds of information collected, as alleged here. For example, in *Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 U.S. Dist. LEXIS 230732, at *1-2, *5 (N.D. Cal. Dec. 22, 2022), the Court declined to find a violation of California's wiretap statute where the defendant used software to "record [the plaintiff's] keystrokes and clicks on the website, while also recording data regarding the date and time of her visit, her browser and operating system, and her geographic location" because the defendant (the website owner) was the "intended recipient of plaintiff's communication." The same result should follow here, where after Plaintiff opened an email *from* Saks, the intended recipient of the read receipt was also Saks.

C. Plaintiff Cannot Reconcile Her Expansive Interpretation of the Arizona Statute with its Actual Legislative History

Plaintiff's expansive reading of the Arizona Statute contradicts the Statute's legislative intent and legislative history. Where, as here, the question is one of first impression under Arizona law, courts in Arizona have looked to the legislative history of a statute at issue, as well as other jurisdictions' resolution of the questions. *See Gila River Indian Cmty. v. Dep't of Child Safety*, 238 Ariz. 531, 534 (Ariz. Ct. App. 2015); *see also Drucker v. Greater Phoenix Transp. Co.*, 197 Ariz. 41, 43 (Ariz. Ct. App. 1999) ("When legislative intent cannot be determined from the exact language of a particular statute, we must consider other things such as context, subject matter, the statute's effect and consequences, reason, and the spirit and purpose of the law.").

The Arizona Statute was first enacted to respond to concerns over pretexting and to address whether additional security was needed to prevent unauthorized disclosure of information that was held by telecommunications companies (*see* H.B. 2785 Summ. 47th Leg., 2d Reg. Sess. (Ariz. Apr. 24, 2006)), and to prohibit the procurement of telephone records by fraudulent, deceptive or false means. *See* H.B. 2785, 47th Leg., 2d Reg. Sess. (Ariz. 2006) (enacted). Although the 2007

amendment included "communication service records," the amendment itself remained rooted in a concern over pretexting (*i.e.*, "the practice of getting personal information under false pretenses"). *See* H.B. 2726 Summ., 48th Leg., 1st Reg. Sess. (Ariz. Mar. 2, 2007).

In the 17 years since its enactment, no court has interpreted the Arizona Statute in the expansive way Plaintiff suggests here. Very few cases address the Arizona Statute at all, and those few cases that do arise in the criminal context. These cases discuss the statutory exception for law enforcement agencies in connection with the performance of their official duties, which suggests that the Arizona Statute contemplated preventing non law-enforcement individuals and entities from deceptively utilizing law-enforcement type tools to collect certain information.

Moreover, that the Arizona legislature has had seventeen years to amend the Arizona Statute to include the type of information the FAC discusses is indicative of its intent not to expand the statute. *See, e.g.*, *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1080 (C.D. Cal. 2023) (concluding that California's wiretap statute could not be expanded to include smart phones and communications over the internet); *see also Rodriguez v. Ford Motor Co.*, No. 3:23-cv-00598-RBM-JLB, 2024 U.S. Dist. LEXIS 50719, at *43-44 (C.D. Cal. Mar. 15, 2024) (collecting cases and declining to adopt plaintiff's extension of the statute to web-based messages sent from the internet browsers of a smartphone, where the statutory text was clear that the statute only applied to communications involving two telephones).

Similarly, in the instant case, the Court should not allow Plaintiff—via one of its several copycat lawsuits—to usurp the role of the Arizona legislature and expand the scope of the Statute. The FAC should be dismissed in its entirety.

CONCLUSION

For the foregoing reasons, Defendant respectfully requests that the Court dismiss all claims asserted against it in this action, with prejudice.

Dated: New York, New York
June 7, 2024

LOEB & LOEB LLP

By: */s/ Christopher A. Ott*

Christopher A. Ott (admitted *pro hac vice*)
901 New York Avenue NW
Suite 300 East
Washington, DC 20001
Tel: (202) 618-5000

Christian D. Carbone
Elena De Santis
345 Park Avenue
New York, NY 10154
Tel: (212) 407-4000

Attorneys for Defendant Saks.com LLC

238533916